Chapter XXXVII
Practical Measures for Securing Government Networks

Stephen K. Aikins
University of South Florida, USA

INTRODUCTION

The modern network and Internet security vulnerabilities expose state and local government networks to numerous threats such as denial of service (DoS) attacks, computer viruses, unauthorized access, confidentiality breaches, and so forth. For example, in June 2005, the state of Delaware saw a spike of 141,000 instances of "suspicious activity" due to a variant of the mytopb worm, which could have brought the state's network to its knees had appropriate steps not been taken (Jarrett, 2005; National Association of State Chief Information Officers [NASCIO], 2006b). On an average day, the state of Michigan blocks 22,059 spam e-mails, 21,702 e-mail viruses, 4,239 Web defacements, and six remote computer takeover attempts. Delaware fends off nearly 3,000 attempts at entering the state's network daily (NASCIO, 2006b).

Governments have the obligation to manage their information security risks by securing mission-critical internal resources such as financial records and taxpayer sensitive information on their networks. Consequently, public-sector information security officers are faced with the challenge to contain damage from compromised systems, prevent internally and Internet-launched attacks, provide systems for logging and intrusion detection, and build frameworks for administrators to securely manage government networks (Oxlenhandler, 2003). This chapter discusses some of the cost-effective measures needed to address government agency information security vulnerabilities and related threats.

BACKGROUND

At the 2005 midyear conference of the National Association of State Chief Information Officers, 89% of responding CIOs polled ranked security among their top three most important issues. However, information technology security initiatives often must compete with other IT resource demands that appear to provide more tangible and immediate business value. The funding and resource constraints facing many state and local governments make it imperative to design and implement an information security model that takes into account the necessary steps and control measures that provide basic information security at the most cost-effective means. Implementing such a security model implies going beyond the

obvious items such as physical security, routers, firewalls, and antivirus, and looking at several other important issues, which include confidentiality, data integrity, content filtering, and incidence response.

In many ways, a government data network will be designed and constructed in a similar manner as any other business data network. However, unlike any private-sector organization, most government agencies do not have the resources to implement overly expensive network architecture. A cost-effective means of securing a public network begins with the documentation of a security policy that reflects the goals of the agency: a realistic assessment of the risks faced by the agency and identification of the resources (manpower, hardware, budget) that are available (Oxlenhandler, 2003). A state or local government agency can manage its network risks by balancing the need for security and cost effectiveness through information security decisions that restrict access to its network, protect against viruses, control network traffic, and provide information assurance within the confines of the available funding structure.

MANAGING GOVERNMENT NETWORK SECURITY RISKS

Physical Security

As a basic means of securing its information resources, a state or local government agency should be able to restrict access to its network hardware. This includes having a data center with access cards to prevent the bad "guys from having unrestricted physical access to systems" (Microsoft Corporation, 2003), and having other physical devices such as routers hopefully located within a wiring closet.

Routers play a key role by transferring and routing all the data communication across the network in a proper mode. Each router maintains a routing table and address resolution protocol (ARP) cache. ARP caches are mappings that correlate an IP (Internet protocol) address to a media access control (MAC) address (Ruth, Hudson, & Microsoft Corporation, 2003). The use of crypto-capable routers will help provide connectivity with the ability of session encryption, thereby preventing the snooping of network traffic. A government agency can use internal routers to segment the organization network into smaller networks for security reasons, such as isolating networks from each other, and for performance reasons such as increasing available routes for data to travel and increasing bandwidth for users. In addition, border routers could also be used to connect to the local government's Internet service provider (Pastore, 2003).

In addition to physical security for the routers, a government agency should maintain up-to-date network configuration documentation and ensure that logical configurations within the routers, firewalls, and servers are not open to attack and possibly compromised. This can be achieved by keeping up to date with vendor patches and ensuring there are complex administrative passwords and settings as hackers usually scan and probe networks for insecure factory-default passwords and settings (McClure, Scambray, & Kurtz, 2002; Ruth et al., 2003).

Antivirus Protection

One concern that every data network, both governmental and private, needs to address is the issue of antivirus protection. Over the past couple of years, much of the damage done to many networks has been caused by virus attacks. For any antivirus network software development, local or state government agencies can focus on a comprehensive solution that addresses the desktop, server, gateway, firewall, and e-mail servers, for example. This defense-in-depth approach is essential as government agencies cannot trust the desktop solution 100%. Desktops must be kept up to date and protected at all times with the antivirus product that is managed centrally for control. As part of its comprehensive security management program, the state of Michigan installed software that filters spam and serves as antivirus solution for incoming and outgoing e-mail. Through this solution, the state stopped monthly averages of